AMENDED IN SENATE AUGUST 7, 2006

AMENDED IN SENATE JUNE 21, 2006

CALIFORNIA LEGISLATURE—2005–06 REGULAR SESSION

# ASSEMBLY BILL No. 2505

**Introduced by Assembly Member Nunez**

February 23, 2006

An act to *amend Section 1798.82 of, and to* add Sections 1798.29.5 and 1798.82.5 to the Civil Code, and to add Chapter 7 (commencing with Section 11770) to Part 1 of Division 3 of Title 2 of the Government Code, relating to information technology.

LEGISLATIVE COUNSEL'S DIGEST

AB 2505, as amended, Nunez. Information technology: privacy: California Information Security Response Team.

(1) Existing law regulates the maintenance and dissemination of personal information by state agencies, as defined, and requires each agency to keep an accurate account of disclosures made pursuant to specified provisions. Existing law requires a state agency, or a person or business that conducts business in California, that owns or licenses computerized data that includes specified personal information to notify any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person because of a breach of the security of the data.

*Existing law permits a state agency, or a person or business that conducts business in California, to provide substitute notice, as defined, to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person because of a breach of the security of the*

*data, when the person or business demonstrates that the costs of providing notice, as defined, would exceed $250,000, or if the number of persons to be notified exceeds 500,000, or if the person or business does not have sufficient contact information.*

*This bill would define substitute notice to include notification to the Office of Privacy Protection.*

~~This bill would require an agency, or a person or business that conducts business in California, to notify the Office of Privacy Protection in the Department of Consumer Affairs whenever notifications to residents of California because of a breach of security are made.~~

(2) Existing law sets forth the duties and authority of various state agencies with respect to information technology activities in the state.

This bill would establish the California Information Security Response Team in state government, with a specified membership chaired by the state chief information officer. The bill would require the California Highway Patrol, upon receiving notification of any information security information incident or computer-related crime, as described, to notify the state chief information officer, who would be required to convene the team to ensure that specified activities have been carried out under existing organizational frameworks, and would require state agencies to cooperate with the team in this regard.

The bill would require the state chief information officer to compile and report to the Legislature no later than December 31, 2007, and annually thereafter, all information security incidents or computer-related crimes reported to the California Highway Patrol.

Vote: majority. Appropriation: no. Fiscal committee: yes. State-mandated local program: no.

*The people of the State of California do enact as follows:*

SECTION 1. Section 1798.29.5 is added to the Civil Code, to read:

1798.29.5. An agency shall notify the Office of Privacy Protection in the Department of Consumer Affairs whenever notifications required under Section 1798.29 are made.

~~SEC. 2. Section 1798.82.5 is added to the Civil Code, to read:~~

~~1798.82.5. A person or business that conducts business in California shall notify the Office of Privacy Protection in the~~

~~Department of Consumer Affairs whenever notifications required under Section 1798.82 are made.~~

*SEC. 2. Section 1798.82 of the Civil Code, as added by Section 4 of Chapter 1054 of the Statutes of 2002, is amended to read:*

1798.82. (a) Any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(d) For purposes of this section, “breach of the security of the system” means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(e) For purposes of this section, “personal information” means an individual’s first name or first initial and last name in

combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

(1) Social security number.

(2) Driver's license number or California Identification Card number.

(3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(f) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(g) For purposes of this section, "notice" may be provided by one of the following methods:

(1) Written notice.

(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.

(3) Substitute notice, if the person or business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the person or business does not have sufficient contact information. Substitute notice shall consist of all of the following:

(A) E-mail notice when the person or business has an e-mail address for the subject persons.

(B) Conspicuous posting of the notice on the Web site page of the person or business, if the person or business maintains one.

(C) Notification to major statewide media *and the Office of Privacy Protection*.

(h) Notwithstanding subdivision (g), a person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part, shall be deemed to be in compliance with the notification requirements of this section if the person or business notifies subject persons in accordance with its policies in the event of a breach of security of the system.

*SEC. 3. Section 1798.82 of the Civil Code, as added by Section 4 of Chapter 915 of the Statutes of 2002, is amended to read:*

1798.82. (a) Any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(d) For purposes of this section, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(e) For purposes of this section, "personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data

elements, when either the name or the data elements are not encrypted:

(1) Social security number.

(2) Driver's license number or California Identification Card number.

(3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(f) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(g) For purposes of this section, "notice" may be provided by one of the following methods:

(1) Written notice.

(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.

(3) Substitute notice, if the person or business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the person or business does not have sufficient contact information. Substitute notice shall consist of all of the following:

(A) E-mail notice when the person or business has an e-mail address for the subject persons.

(B) Conspicuous posting of the notice on the Web site page of the person or business, if the person or business maintains one.

(C) Notification to major statewide media *and the Office of Privacy Protection*.

(h) Notwithstanding subdivision (g), a person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part, shall be deemed to be in compliance with the notification requirements of this section if the person or business notifies subject persons in accordance with its policies in the event of a breach of security of the system.

~~SEC. 3.~~

*SEC. 4.* Chapter 7 (commencing with Section 11770) is added to Part 1 of Division 3 of Title 2 of the Government Code, to read:

## Chapter 7. California Information Security Response Team

11770. (a) The California Information Security Response Team is hereby established in state government.

(b) The team shall consist of the following members:

(1) The state chief information officer, who shall act as chair.

(2) The Assistant Chief of the Office of Technology Review, Oversight, and Security in the Department of Finance, also known as the state information security officer.

(3) The Director of Technology Services.

(4) The Director of the Office of Privacy Protection in the Department of Consumer Affairs.

(5) The director of the California Highway Patrol's Emergency Notification and Tactical Alert Center.

11771. (a) Upon receiving notification as required by the Department of Finance of any information security incident or computer-related crimes, as described in the State Administrative Manual or subdivision (c) of Section 502 of the Penal Code, the California Highway Patrol shall notify the state chief information officer, who shall convene the California Information Security Response Team to ensure that all of the following have occurred under existing organizational frameworks:

(1) That technical assistance is provided to state agencies to resolve security issues and address any potential disruption of state computer services.

(2) That all potential computer crimes and criminal security incidents are properly investigated.

(3) That the provisions of Section 1798.29 of the Civil Code are followed in a timely manner.

(b) State agencies shall cooperate in providing information to the team in the implementation of subdivision (a), as requested.

11772. The state chief information officer shall compile and report to the Legislature no later than December 31, 2007, and annually thereafter, all information security incidents or

computer-related crimes reported to the California Highway Patrol. The report shall generally describe the type of reported security breach, or potential security breach, and the response provided.

O